

CLAIMS:

1. A secure communication method, comprising
generating an Internet Protocol request from a client apparatus destined for a target server;
receiving the Internet Protocol request at an intermediate server;
sending an Internet Protocol request for authentication information from the intermediate server to the client apparatus;
sending the requested authentication information from the client apparatus to the intermediate server;
performing a validation check on the authentication information; and
transparently passing on the Internet Protocol request from the client apparatus to the target server and returning data from the target server to the client apparatus dependent upon the outcome of the validation.
2. A secure communication method according to claim 1 wherein the received Internet Protocol request is acknowledged by the intermediate server to the client apparatus, the client apparatus responds with an acknowledgement including an identifier that the client apparatus may be authorised to access the target server, the request for authentication information is only sent when the identifier is received by the intermediate server, and a default response is sent by the intermediate server to the client apparatus if the identifier is not received by the intermediate server.
3. A secure communication method according to claim 2 wherein the default response is a message that data requested by the Internet Protocol request was not found.
4. A secure communication method according to claim 2 wherein the default response is default data.
5. A secure communication method according to claim 1 wherein the target server has a class 3 Internet Protocol address and Internet Protocol communication between the intermediate server and the target server is over a local area network.

6. A secure communications method according to claim 1 wherein the validation is performed at a validation server upon a validation request from the intermediate server.
7. A secure communication method according to claim 6 wherein the secure server has a class 3 Internet Protocol address and Internet Protocol communication between the intermediate server and the secure server is over a local area network.
8. A secure communication method according to claim 6 wherein the secure server includes a database of authorised users for the performance of the validation.
9. A secure communication method according to claim 8 wherein the secure server also includes a potential users database if the validation procedure is unsuccessful the received authentication information is entered in the potential users database, and an administrator can transfer the authentication information for a user from the potential users database to the valid users database.
10. A secure communication method according to claim 1 wherein the Internet Protocol request is generated with the domain name given for the target server, and the domain name is converted to the Internet Protocol address of the intermediate server by a Domain Name Server.
11. A secure communication method according to claim 10 wherein the Internet Protocol address of the intermediate server is a class A or B address.
12. A secure communications method according to claim 1 wherein the authentication information includes client apparatus information uniquely identifying hardware and/or software of the client apparatus.
13. A secure communication method according to claim 1 wherein the authentication information includes an electronically generated serial number.

14. A secure communication method according to claim 1 wherein a user of the client apparatus enters a username and password and the authentication information includes the username and password.

15. A secure communication method according to claim 1, wherein if the validation procedure fails a default response is sent to the client apparatus by the intermediate server.

16. A secure communication method according to claim 14 wherein the default response is default data.

17. A secure communication method according to claim 15 wherein the default response is a message that data requested by the Internet Protocol request was not found or available or that access is denied.

18. A secure communication method according to claim 1 wherein if no authentication information is received within a predetermined time period by the intermediate server from the client apparatus, a default response is sent to the client apparatus by the intermediate server.

19. A secure communication method according to claim 18 wherein the default response is a message that data requested by the Internet Protocol request was not found or available or that access is denied.

20. A secure communication method according to claim 18 wherein the default response is default data.

21. A secure communication system comprising:

RECEIVED 5041660

a client apparatus having an application for generating an Internet Protocol request destined for a target server, and an authentication application for sending authentication information to an intermediate server; and

an intermediate server having an application for receiving the Internet Protocol request, for sending an Internet Protocol request for authentication information to the client apparatus, for receiving authentication information, for performing a validation process for the authentication information, and for transparently passing on the Internet Protocol request from the client apparatus to the target server and returning data from the target server to the client apparatus dependent upon the outcome of the validation process.

22. A secure communication system, according to claim 21 wherein the application of the intermediate server is operative to acknowledge the received Internet Protocol request to the client apparatus; the application of the client apparatus is operative to respond with an acknowledgement including an identifier that the client apparatus may be authorised to access the target server; and the application of the intermediate server is operative to only send the request for authentication information when the identifier is received by the intermediate server; and to send a default response to the client apparatus if the identifier is not received.

23. A secure communication system according to claim 22 wherein the default response is a message that data requested by the Internet Protocol request was not found or available or that access is denied.

24. A secure communication system according to claim 22 wherein the default response is default data.

25. A secure communication system according to claim 21 wherein the target server has a class 3 Internet Protocol address and Internet Protocol communication between the intermediate server and the target server is over a local area network.

26. A secure communication system according to claim 21 including a validation server, for receiving a validation request from the intermediate server for performing a validation check and for sending a validation result to the intermediate server, wherein the application of the intermediate server is operative to perform the validation process by sending the validation request to the validation server and receiving the validation result.

27. A secure communication system according to claim 26 wherein the secure server has a class 3 Internet Protocol address and Internet Protocol communication between the intermediate server and the secure server is over a local area network.

28. A secure communication system according to claim 26 wherein the secure server includes a database of authorised users for the performance of the validation.

29. A secure communication system according to claim 28 wherein the secure server also includes a potential users database; the secure server being operative, if the validation check is unsuccessful, to enter the received authentication information in the potential users database; the secure server also including an administrator interface to allow an administrator to transfer the authentication information for a user from the potential users database to the valid users database.

30. A secure communication system according to claim 21, wherein the application of the client apparatus is operative to generate the Internet Protocol request with the domain name given for the target server, and the domain name is converted to the Internet Protocol address of the intermediate server by a Domain Name Server.

31. A secure communication system according to claim 30 wherein the Internet Protocol address of the intermediate server is a class A or B address.

32. A secure communication system according to claim 21 wherein the authentication information includes client apparatus information uniquely identifying hardware and/or software of the client apparatus.
33. A secure communication system according to claim 21 wherein the authentication information includes an electronically generated serial number.
34. A secure communication system according to claim 21 wherein the client apparatus receives a username and password from a user and the authentication information includes the username and password.
35. A secure communication system according to claim 21 wherein the application of the intermediate server is operative to, if the validation process is negative, send a default response to the client apparatus.
36. A secure communication system according to claim 35 wherein the default response is default data.
37. A secure communication system according to claim 35 wherein the default response is a message that data requested by the Internet Protocol request was not found or available or that access is denied.
38. A secure communication system according to claim 21 wherein the authentication server is operative to, if no authentication information is received within a predetermined period of time from the client apparatus, send a default response to the client apparatus.
39. A secure communication system according to claim 38 wherein the default response is a message that data requested by the Internet Protocol request was not found or available or that access is denied.

40. A secure communication system according to claim 38 wherein the default response is default data.

41. A server apparatus for providing secure communication over a communications network using Internet Protocol, to a target server from a client apparatus, the server apparatus comprising:

an interface for connecting the client apparatus over the network for receiving an Internet Protocol request from the client apparatus destined for the target server, for sending a request for authentication information to the client apparatus, and for receiving the requested authentication information;

validation means for performing a validation process for the authentication information; and

routing means for passing on the Internet Protocol request from the client apparatus to the target server and returning data from the target server to the client apparatus dependent upon the outcome of the validation process.

42. A server apparatus according to claim 41 wherein said interface is adapted to acknowledge the received Internet Protocol request to the client apparatus, to receive an acknowledgement from the client apparatus, including an identifier that the client apparatus may be authorised to access the target server, and to send to the client apparatus the request for authentication information when the identifier is received or a default response when the identifier is not received.

43. A server apparatus according to claim 42 wherein the default response is a message that data requested by the Internet Protocol request was not found or available or that access is denied.

44. A server apparatus according to claim 42 wherein the default response is default data.

45. A server apparatus according to claim 41 wherein said routing means includes a local area network interface for communication with the target server using a class 3 Internet Protocol address for the target server.
46. A server apparatus according to claim 41 wherein the validation means is operative to send a validation request to a validation server and to receive a validation result.
47. A server apparatus according to claim 46 wherein the validation means includes a local area network interface means for communication with the secure server using a class 3 Internet Protocol address for the secure server.
48. A server apparatus according to claim 41 wherein the interface has a class A or B Internet Protocol Address.
49. A server apparatus according to claim 41 wherein the interface is adapted to send a default response to the client apparatus if the validation process is unsuccessful.
50. A server apparatus according to claim 49 wherein the default response is a message that data requested by the Internet Protocol request was not found or available or that access is denied.
51. A server application according to claim 49 wherein the default response is default data.
52. A server apparatus according to claim 41 wherein the interface is adapted to send a default response to the client apparatus if not authentication information is received within a predetermined time period.

53. A server apparatus according to claim 52 wherein the default response is a message that data requested by the Internet Protocol request was not found or available or that access is denied.

54. A server apparatus according to claim 52 wherein the default response is default data.

55. A method of operating a security server for providing secure access to a target server by a client apparatus over a communication network using Internet Protocol, the method comprising:

receiving an Internet Protocol request from the client apparatus destined for the target server;

sending an Internet Protocol request for authentication information to the client apparatus;

receiving the requested authentication information;

performing a validation process for the authentication information; and

passing on the Internet Protocol request from the client apparatus to the target server and returning data from the target server to the client apparatus dependent upon the outcome of the validation process.

56. A method according to claim 55 including acknowledging the received Internet Protocol request to the client apparatus, receiving an acknowledgement from the client apparatus including an identifier that the client apparatus may be authorised to access the target server, and sending to the client apparatus the request for authentication information when the identifier is received or a default response when the identifier is not received.

57. A method according to claim 56 wherein the default response is a message that data requested by the Internet Protocol request was not found or available or that access is denied.

58. A method according to claim 56 wherein the default response is default data.
59. A method according to claim 55 wherein the target server has a class 3 Internet Protocol address and Internet Protocol communication with the target server are made using a local area network.
60. A method according to claim 55 wherein the validation process comprises sending a validation request to a validation server and receiving a validation result from the validation server.
61. A method according to claim 60 wherein the secure server has a class 3 Internet Protocol address and Internet Protocol communications with the secure server are made using a local area network.
62. A method according to claim 55 wherein Internet Protocol address used for the security server for Internet Protocol communications with the client apparatus is a class A or B address.
63. A method according to claim 55 wherein a default response is sent to the client apparatus if the validation process is unsuccessful.
64. A method according to claim 63 wherein the default response is a message that data requested by the Internet Protocol request was not found or available or that access is denied.
65. A method according to claim 63 wherein the default response is default data.
66. A method according to claim 55 wherein a default response is sent to the client apparatus if no authentication information is received within a predetermined time period.

67. A method according to claim 66 wherein the default response is a message that data requested by the Internet Protocol request was not found or available or that access is denied.
68. A method according to claim 66 wherein the default response is default data.
69. A security server for providing secure access to a target server by a client over an Internet Protocol network, the server comprising:
- an Internet Protocol interface for connection to the client over said network;
 - an interface for connection to said target server;
 - program memory for storing program code for controlling a processor; and
 - a processor for implementing the stored program code, to control the interface;
- wherein the program code comprises code to control the processor to:
- receive an Internet Protocol request from the client destined for the target server;
 - send an Internet Protocol request for authentication information to the client;
 - receive the requested authentication information;
 - perform a validation process for the authentication information; and
 - pass on the Internet Protocol request from the client to the target server and return data from the target server to the client dependent upon the outcome of the validation process.
70. A client apparatus for gaining a validated access to data at a target server over an Internet Protocol network, the client apparatus comprising:
- an interface to the Internet Protocol network for sending an Internet Protocol request destined for the target server, for receiving an Internet Protocol request for authentication information from a security server, and for sending the requested authentication information to the security server using the Internet Protocol; and
 - authentication means for generating the authentication information;
- wherein the interface is arranged to receive data from the target server if authentication of the authentication information is successful.

71. A client apparatus according to claim 70 wherein the authentication means is adapted to generate the authentication information to include information uniquely identifying hardware and/or software of the client apparatus.
72. A client apparatus according to claim 70 wherein the authentication means is adapted to generate the authentication information to include an electronically generated serial number.
73. A client apparatus according to claim 70 including user interface means for allowing a user to input a username and a password, wherein the authentication means is adapted to generate the authentication information to include the username and password.
74. A client apparatus according to claim 70 including an application for generating the Internet Protocol request and for using received data, wherein the interface includes means for monitoring and modifying Internet Protocol packets passing between the Internet Protocol network and the application.
75. A method of controlling a client apparatus for gaining a validated access to data at a target server over an Internet Protocol network, the method comprising:
- sending an Internet Protocol request destined for the target server;
 - receiving an Internet Protocol request for authentication information from a security server;
 - generating authentication information;
 - sending the authentication information to the security server using the Internet Protocol; and
 - receiving data from the target server if authentication of the authentication information is successful.

27

76. A method according to claim 75 wherein the authentication information is generated to include information uniquely identifying hardware and/or software of the client apparatus.

77. A method according to claim 75 wherein the authentication information is generated to include an electronically generated serial number.

78. A method according to claim 75 wherein a username and a password are input, and the authentication information is generated to include the username and password.

79. A method according to claim 75 including generating an Internet Protocol request using an application, and Internet Protocol packets passing between the Internet Protocol network and the application are monitored and modified to send the requested authentication information to the security server.

80. A carrier medium carrying computer readable code for controlling a processing apparatus to implement the method of any one of claims 55, to 68 or 75 to 79.

81. A secure communication method, comprising
generating an packet routing layer protocol request from a client destined for a target server;
receiving the packet routing layer protocol request at an intermediate server;
sending an packet routing layer protocol request for authentication information from the intermediate server to the client;
sending the requested authentication information from the client to the intermediate server;
performing a validation check on the authentication information; and
transparently passing on the packet routing layer protocol request from the client to the target server and returning data from the target server to the client in dependence upon the outcome of the validation.

5

82. A secure communication system comprising:

a client having an application for generating a packet routing layer protocol request destined for a target server, and an authentication application for sending authentication information to an intermediate server; and

an intermediate server having an application for receiving the packet routing layer protocol request, for sending an packet routing layer protocol request for authentication information to the client, for receiving authentication information, for performing a validation process for the authentication information, and for transparently passing on the packet routing layer protocol request from the client to the target server and returning data from the target server to the client dependent upon the outcome of the validation process.

83. A server for providing secure communication over a communications network using a packet routing layer protocol, to a target server from a client, the server comprising:

an interface for connecting the client over the network for receiving an packet routing layer protocol request from the client destined for the target server, for sending a request for authentication information to the client, and for receiving the requested authentication information;

validation means for performing a validation process for the authentication information; and

routing means for passing on the packet routing layer protocol request from the client to the target server and returning data from the target server to the client in dependence upon the outcome of the validation process.

84. A security server for providing secure access to a target server by a client over a packet routing layer protocol network, the server comprising:

a packet routing layer protocol interface for connection to the client over said network;

an interface for connection to said target server;

program memory for storing program code for controlling a processor; and

29

a processor for implementing the stored program code, to control the interface;
wherein the program code comprises code to control the processor to:
receive an packet routing layer protocol request from the client destined for the
target server;
send an packet routing layer protocol request for authentication information to
the client;
receive the requested authentication information;
perform a validation process for the authentication information; and
pass on the packet routing layer protocol request from the client to the target
server and return data from the target server to the client dependent upon the outcome of
the validation process.

85. A client for gaining a validated access to data at a target server over a network
using a packet routing layer protocol, the client comprising:
an interface to the network for sending an packet routing layer protocol request
destined for the target server, for receiving an packet routing layer protocol request for
authentication information from a security server, and for sending the requested
authentication information to the security server using the packet routing layer protocol;
and
authentication means for generating the authentication information;
wherein the interface is arranged to receive data from the target server if
authentication of the authentication information is successful.

86. A method of operating a security server for providing secure access to a target
server by a client over a communication network using a packet routing layer protocol,
the method comprising:
receiving a packet routing layer protocol request from the client destined for the
target server;
sending a packet routing layer protocol request for authentication information to
the client;
receiving the requested authentication information;

performing a validation process for the authentication information; and
passing on the packet routing layer protocol request from the client to the target server and returning data from the target server to the client dependent upon the outcome of the validation process.

87. A method of controlling a client for gaining a validated access to data at a target server over a network using a packet routing layer protocol, the method comprising:

sending an packet routing layer protocol request destined for the target server;
receiving an packet routing layer protocol request for authentication information from a security server;
generating authentication information;
sending the authentication information to the security server using the packet routing layer protocol; and
receiving data from the target server if authentication of the authentication information is successful.

88. A carrier medium carrying computer readable code for controlling a processing apparatus to implement the method of any one of claims 81, 86 or 87.